



# **Podręcznik zarządzania komputerami typu desktop**

## **Komputery Business PC**

Numer katalogowy dokumentu: 391759-241

**Maj 2005 r.**

W tym podręczniku zawarte są definicje i instrukcje dotyczące korzystania z funkcji zabezpieczeń oraz systemu inteligentnego zarządzania Intelligent Manageability, które są zainstalowane fabrycznie na niektórych modelach komputerów.

© Copyright 2005 Hewlett-Packard Development Company, L.P.  
Informacje zawarte w niniejszym dokumencie mogą zostać zmienione bez  
uprzedzenia.

Microsoft oraz Windows są znakami towarowymi firmy Microsoft Corporation  
w USA i w innych krajach.

Jedynie warunki gwarancji na produkty i usługi firmy HP są ujęte  
w odpowiednich informacjach o gwarancji towarzyszących tym produktom  
i usługom. Żadne z podanych tu informacji nie powinny być uznawane za  
jakikolwiek gwarancje dodatkowe. Firma HP nie ponosi odpowiedzialności za  
błędy techniczne lub wydawnicze ani pominięcia, jakie mogą wystąpić  
w tekście.

Niniejszy dokument zawiera prawnie zastrzeżone informacje, które są  
chronione prawami autorskimi. Żadna część tego dokumentu nie może być  
fotokopiowana, reprodukowana ani tłumaczona na inny język bez uprzedniej  
pisemnej zgody firmy Hewlett-Packard.



**OSTRZEŻENIE:** Tak oznaczane są zalecenia, których nieprzestrzeganie  
może doprowadzić do obrażeń ciała lub śmierci.

---



**PRZESTROGA:** Tak oznaczane są zalecenia, których nieprzestrzeganie  
może doprowadzić do uszkodzenia sprzętu lub utraty danych.

---

## **Podręcznik zarządzania komputerami typu desktop**

Komputery Business PC

Wydanie pierwsze (Maj 2005 r.)

**Numer katalogowy dokumentu: 391759-241**

---

# Spis treści

## Podręcznik zarządzania komputerami typu desktop

Początkowa konfiguracja i rozmieszczanie.....	2
Altiris Deployment Solution Agent .....	3
HP Local Recovery .....	3
Zdalne instalowanie systemu.....	4
Aktualizowanie oprogramowania	
i zarządzanie nim.....	5
HP System Software Manager .....	5
HP Client Manager Software .....	6
HP Client Management Solutions using Altiris .....	7
HP OpenView Management Suite for Desktops Using Radia .....	9
HP Local Recovery .....	10
Dantz Retrospect Express .....	12
Proactive Change Notification .....	13
Subscriber's Choice .....	14
Wycofane rozwiązania .....	14
Pamięć ROM typu flash .....	15
Zdalne zarządzanie pamięcią ROM typu flash.....	16
HPQFlash .....	16
Tryb awaryjnego odzyskiwania bloku rozruchowego .....	16
Replikowanie ustawień konfiguracyjnych .....	18
Dwufunkcyjny przycisk zasilania.....	27
Witryna sieci Web .....	28
Współpraca z innymi producentami.....	28
Śledzenie i zabezpieczanie majątku .....	29
Zabezpieczanie hasłem .....	34
Ustawianie hasła konfiguracyjnego za pomocą programu Computer Setup.....	35
Ustawianie hasła uruchomieniowego za pomocą programu Computer Setup .....	36
Blokada DriveLock.....	41
Czujnik Smart Cover Sensor.....	43

Smart Cover Lock . . . . .	45
Zabezpieczająca blokada kablowa . . . . .	47
Identyfikacja na podstawie analizy linii papilarnych . . . . .	47
Powiadamianie o usterkach i ich usuwanie . . . . .	48
System ochrony dysków . . . . .	48
Zasilacz z zabezpieczeniem antyprzepięciowym . . . . .	48
Czujnik termiczny . . . . .	49

## **Indeks**

---

# Podręcznik zarządzania komputerami typu desktop

System HP Client Management Solutions zawiera oparte na standardach rozwiązania służące do sterowania i sprawowania nadzoru nad komputerami typu desktop, stacjami roboczymi i komputerami przenośnymi w środowisku sieciowym. W 1995 roku firma HP — jako pierwsza w branży — wprowadziła na rynek rodzinę komputerów osobistych typu desktop z zaimplementowaną funkcją zarządzania. Firma HP jest posiadaczem patentu na technologię zarządzania. Od tego czasu prowadzone były — zakrojone na szeroką skalę — prace mające na celu rozwój standardów i infrastruktury, pozwalających na efektywne rozmieszczanie i konfigurowanie komputerów typu desktop, przenośnych i stacji roboczych oraz zarządzanie nimi. W związku z tym podjęto ścisłą współpracę z wiodącymi producentami oprogramowania, co umożliwiło zachowanie zgodności między dostarczonymi przez nich programami a systemem HP Client Management Solutions. System ten jest istotnym elementem prowadzonych działań, których celem jest opracowanie rozwiązań wspomagających decyzje klientów podczas czterech faz cyklu życia komputerów typu desktop — planowania, rozmieszczania, zarządzania i unowocześniania.

Najważniejsze funkcje i możliwości zarządzania komputerami typu desktop to:

- Początkowa konfiguracja i rozmieszczanie
- Zdalne instalowanie systemu
- Aktualizowanie oprogramowania i zarządzanie nim
- Pamięć ROM typu flash
- Śledzenie i zabezpieczanie majątku
- Powiadamianie o usterkach i ich usuwanie



Obsługa poszczególnych funkcji opisanych w tym podręczniku może się różnić w zależności od modelu lub wersji oprogramowania.

---

## Początkowa konfiguracja i rozmieszczanie

Komputer został dostarczony wraz z preinstalowanym obrazem oprogramowania systemowego. Dzięki temu po szybkim „rozpakowaniu” oprogramowania komputer jest gotowy do pracy.

Użytkownik może zastąpić preinstalowany obraz oprogramowania dostosowanym zestawem oprogramowania systemowego i aplikacji. Istnieje kilka metod rozmieszczania takiego oprogramowania. Zostały one wymienione poniżej:

- Zainstalowanie dodatkowych aplikacji po rozpakowaniu preinstalowanego obrazu oprogramowania.
- Zastąpienie preinstalowanego oprogramowania dostosowanym obrazem oprogramowania za pomocą narzędzi rozmieszczania (np. Altiris Deployment Solution).
- Skopiowanie zawartości jednego dysku twardego na inny (w ramach procesu klonowania danych).

Najlepsza metoda rozmieszczania zależy od charakteru środowiska informatycznego oraz realizowanych w nim procesów. Informacje pomocne w wyborze tej metody można uzyskać w części dotyczącej rozmieszczania komputera, dostępnej w witrynie sieci Web poświęconej zalecanym rozwiązaniom i oferowanym usługom (<http://whp-sp-orig.extweb.hp.com/country/us/en/solutions.html>).

Informacje o odzyskiwaniu oprogramowania systemowego, zarządzaniu konfiguracją i energią oraz rozwiązywaniu problemów można znaleźć na dysku CD *Restore Plus!*, a także w dokumentacji dotyczącej programu Computer Setup i sprzętu obsługującego funkcję ACPI.

## Altiris Deployment Solution Agent

Program ten jest wstępnie załadowany na komputerze.  
Po zainstalowaniu umożliwia komunikację z konsolą  
Deployment Solution administratora.

Aby zainstalować program Altiris Deployment Solution Agent:

1. Kliknij przycisk **Start**.
2. Kliknij polecenie **Wszystkie programy**.
3. Kliknij pozycję **Software Setup**.
4. Kliknij przycisk **Next (Dalej)**.
5. Przewiń listę w dół i kliknij łącze instalacji programu  
Altiris AClient.

## HP Local Recovery

Program Local Recovery wykonuje kopie zapasowe danych  
i plików systemowych w chronionym obszarze na dysku twardym.  
W razie utraty, usunięcia bądź uszkodzenia danych lub plików  
program Local Recovery umożliwia ich pobranie lub przywrócenie  
ostatniego dobrego obrazu systemu.

Aby zainstalować ten wstępnie załadowany program:

1. Kliknij przycisk **Start**.
2. Kliknij polecenie **Local Recovery**.
3. Kliknij przycisk **Next (Dalej)**.
4. Przewiń listę w dół i kliknij łącze instalacji programu  
HP Local Recovery.

## Zdalne instalowanie systemu

Funkcja zdalnego instalowania systemu umożliwia uruchomienie i skonfigurowanie systemu operacyjnego za pomocą oprogramowania i informacji konfiguracyjnych znajdujących się na serwerze sieciowym, poprzez zainicjowanie środowiska Preboot Execution Environment (PXE). Funkcja zdalnego instalowania systemu służy zazwyczaj do instalowania i konfigurowania systemu operacyjnego, lecz może również zostać użyta do przeprowadzenia następujących zadań:

- Formatowanie dysku twardego.
- Rozmieszczanie obrazu oprogramowania na jednym lub kilku nowych komputerach.
- Zdalne aktualizowanie systemu BIOS w pamięci ROM typu flash („Zdalne zarządzanie pamięcią ROM typu flash“ na stronie 16).
- Konfigurowanie ustawień systemu BIOS.

Aby rozpocząć proces zdalnego instalowania systemu, należy nacisnąć klawisz **F12** (po pojawieniu się — w prawym dolnym rogu ekranu z logo firmy HP — komunikatu „F12 = Network Service Boot“), a następnie postępować zgodnie z wyświetlanymi instrukcjami. Domyślna kolejność rozruchu jest ustawieniem konfiguracyjnym systemu BIOS, które można zmienić na opcję podejmowania każdorazowo próby uruchomienia środowiska PXE.

Firmy HP oraz Altiris wspólnie opracowały narzędzia pozwalające na łatwiejsze i szybsze przeprowadzanie rozmieszczania komputerów oraz zarządzanie nimi w ramach przedsiębiorstwa. Dzięki znacznemu obniżeniu całkowitych kosztów związanych z wdrożeniem systemu informatycznego, komputery klienckie firmy HP stanowią najodpowiedniejsze — pod kątem zarządzania — rozwiązanie dla przedsiębiorstwa.



## Aktualizowanie oprogramowania i zarządzanie nim

Firma HP oferuje kilka narzędzi służących do zarządzania oprogramowaniem zainstalowanym na komputerach typu desktop, stacjach roboczych i komputerach przenośnych oraz aktualizowania go:

- HP System Software Manager
- HP Client Manager Software
- HP Client Management Solutions using Altiris
- HP OpenView Management Suite for Desktops using Radia
- HP Local Recovery
- Dantz Backup and Recovery
- HP Proactive Change Notification
- HP Subscriber's Choice

### HP System Software Manager

HP System Software Manager (SSM) to bezpłatne narzędzie automatyzujące proces zdalnego rozmieszczania sterowników urządzeń i aktualizacji systemu BIOS na sieciowych komputerach HP Business PC. Oprogramowanie SSM, działając dyskretnie (bez interakcji ze strony użytkownika), określa poziom wersji sterowników i systemu BIOS zainstalowanych w każdym sieciowym systemie klienckim i porównuje te informacje z plikami SoftPaq oprogramowania systemowego, które zostały przetestowane i są przechowywane w centralnym magazynie plików. Następnie program ten aktualizuje wszelkie oprogramowanie systemowe o niższych wersjach na sieciowych komputerach PC do nowszych wersji dostępnych w magazynie plików. Ponieważ program SSM umożliwia dystrybucję aktualizacji SoftPaq tylko na właściwe modele systemów klienckich, administratorzy mogą za jego pomocą utrzymywać aktualność oprogramowania systemowego w sposób pewny i efektywny.

Oprogramowanie System Software Manager integruje się z narzędziami dystrybucji oprogramowania klasy korporacyjnej, takimi jak HP OpenView Management Suite using Radia i Microsoft Systems Management Server (SMS). Za pomocą oprogramowania SSM można rozprowadzać aktualizacje tworzone przez klientów i aktualizacje innych firm, które zostały spakowane w formacie SSM.

Oprogramowanie SSM można pobrać bezpłatnie ze strony [www.hp.com/go/ssm](http://www.hp.com/go/ssm).

## HP Client Manager Software

Oprogramowanie HP Client Manager Software, opracowane wspólnie z firmą Altiris, jest dostępne bezpłatnie dla wszystkich obsługiwanych modeli komputerów HP Business typu desktop, przenośnych i stacji roboczych. Z oprogramowaniem tym jest zintegrowany program SSM, umożliwiając centralne śledzenie i monitorowanie aspektów sprzętowych systemów klienckich HP oraz zarządzanie nimi.

Oprogramowanie HP Client Manager umożliwia:

- Uzyskiwanie cennych informacji dotyczących sprzętu, takiego jak procesor, pamięć, karta wideo i ustawienia zabezpieczeń.
- Monitorowanie kondycji systemu w celu rozwiązywania problemów jeszcze przed ich wystąpieniem.
- Instalowanie aktualizacji sterowników i systemu BIOS bez potrzeby fizycznego dostępu do każdego komputera.
- Zdalne konfigurowanie systemu BIOS i ustawień zabezpieczeń.
- Automatyzowanie procesów w celu szybkiego rozwiązywania problemów związanych ze sprzętem.

Oprogramowanie HP Client Manager używa tej samej infrastruktury firmy Altiris co inne rozwiązania firmy Altiris w zakresie zarządzania cyklem życia systemów klienckich. Konstrukcja taka daje znaczne korzyści personelowi informatycznemu, ponieważ konieczne jest instalowanie i utrzymywanie tylko jednej infrastruktury. Informacje są przechowywane w jednej bazie danych, dzięki czemu możliwe jest uzyskiwanie pełnych i spójnych raportów inwentaryzacyjnych oraz informacji o kondycji i zabezpieczeniach systemu. Do planowania i śledzenia zadań związanych z zarządzaniem sprzętem i oprogramowaniem systemów klienckich używa się jednej spójnej konsoli.

Więcej informacji o oprogramowaniu HP Client Manager można znaleźć na stronie [www.hp.com/go/easydeploy](http://www.hp.com/go/easydeploy).

## HP Client Management Solutions using Altiris

Firma HP oferuje do zakupu dodatkowe rozwiązania firmy Altiris w zakresie zarządzania systemami klienckimi, które uzupełniają możliwości zarządzania sprzętem oferowane przez oprogramowanie HP Client Manager. Te rozwiązania firmy Altiris są nakierowane na wyzwania związane z zarządzaniem cyklem życia systemów klienckich, w tym:

- Szacowanie inwentaryzacyjne
- Zgodność licencji na oprogramowanie
- Migracja osobowości
- Rozmieszczanie obrazu oprogramowania
- Dystrybucja oprogramowania
- Zarządzanie zasobami
- Tworzenie kopii zapasowych klienta i odzyskiwanie go
- Rozwiązywanie problemów

Więcej informacji o rozwiązaniach HP Client Management Solutions using Altiris można znaleźć na stronie [www.hp.com/go/easydeploy](http://www.hp.com/go/easydeploy).

Firmy HP i Altiris prowadzą wyjątkową współpracę na zasadzie partnerstwa, wykraczającą poza sprzedaż i marketing, obejmującą wspólne opracowywanie produktów oraz dzielenie się technologią. Partnerstwo to rozciąga się na grupy HP Client, Server, OpenView i Services, zapewniając najnowocześniejsze rozwiązania partnerom i klientom HP.

Począwszy od 1999 roku, grupa systemów osobistych Compaq i firma Altiris zawarły przymierze w celu połączenia silnych stron firmy Compaq jako pioniera w sprzęcie komputerów osobistych i możliwościach zarządzania z silnymi stronami firmy Altiris w zakresie rozmieszczania i migrowania komputerów osobistych. Związek ten rozwinął się w strategiczne przymierze wraz z wprowadzeniem rozbudowanych i zmniejszających koszty rozwiązań w zakresie zarządzania cyklem życia IT, w tym opracowanego wspólnie oprogramowania HP Client Manager Software, który zapewnia najbardziej zaawansowane możliwości zarządzania komputerami osobistymi firmy HP.

W oparciu o sukces grupy systemów osobistych, w 2001 roku grupa serwerów będących standardem przemysłowym wprowadziła oprogramowanie ProLiant Essentials Rapid Deployment Pack — wersję OEM narzędzia Altiris Deployment Solution połączonego z zestawem SmartStart Toolkit firmy HP. Firma HP stosuje to rozwiązanie do zaopatrzenia serwerów ProLiant (w tym serwerów typu blade), jak również komputerów osobistych typu blade, najważniejszego składnika rozwiązania Consolidated Client Infrastructure firmy HP.

Po połączeniu firm HP i Compaq partnerstwo było nadal rozszerzane o następujące oferty:

- Narzędzie Altiris Deployment Solution jest dostępne bezpłatnie jako 30-dniowa wersja próbna dla komputerów HP Business PC, a po okresie tym można nabyć licencję.
- HP Local Recovery — narzędzie tworzenia kopii zapasowych/odzyskiwania komputerów klienckich — jest dostępne bezpłatnie z komputerami HP Business PC.
- Altiris Connector for HP OpenView zapewnia inwentaryzację klienta oraz integrację zdarzeń z produktami HP OpenView Network Node Manager, Operations i Service Desk.
- Altiris Connector for HP Systems Insight Manager umożliwia skonsolidowane rozmieszczanie serwerów i klientów HP oraz zarządzanie nimi z poziomu konsoli HP Systems Insight Manager.

Firma HP jest liderem na rynku, oferując pojedyncze rozwiązanie zarządzające i konsolę służącą do rozmieszczania i konfigurowania komputerów osobistych, kieszonkowych, typu thin client oraz serwerów z systemem Windows i Linux, jak również rozbudowaną integrację z narzędziami HP do zarządzania dla przedsiębiorstw. Firma HP oferuje obszerne szkolenia oraz wiedzę w zakresie usług udostępniane przez organizację HP Services i firmę Altiris. To połączenie systemu HP Client Management Solutions oraz możliwości usług zapewnia najlepszy wybór dla klientów dążących do zmniejszenia kosztów i złożoności zarządzania systemami klienckimi.

## HP OpenView Management Suite for Desktops Using Radia

HP OpenView Management Suite for Desktops using Radia to wysoce skalowalne, oparte na zasadach oprogramowanie do zarządzania zmianami i konfiguracją, które umożliwia administratorom efektywne i niezawodne prowadzenie inwentaryzacji, rozmieszczanie i utrzymywanie oprogramowania oraz zawartości na heterogonicznych platformach typu desktop z poziomu konsoli opartej na sieci Web.

Oprogramowanie HP OpenView Management Suite for Desktops using Radia zapewnia dostępność aplikacji i gwarantuje, że systemy operacyjne, aplikacje i zawartość potrzebne pracownikom, partnerom lub klientom są w 100% właściwe — przez cały czas.

Oprogramowanie HP OpenView Management Suite for Desktops using Radia zostało uznane przez klientów korporacyjnych na całym świecie jako rozwiązanie zapewniające ponad 99% niezawodność rozmieszczania w wysoce złożonych i dużych środowiskach IT. Automatyzuje ono zarządzanie zmianami, powodując znaczne oszczędności kosztów IT, przyspieszony czas wprowadzenia na rynek dla oprogramowania i zawartości, a także zwiększoną wydajność użytkownika i jego zadowolenie.

Oprogramowanie HP OpenView Management Suite for Desktops umożliwia informatykom wykonywanie następujących zadań:

- Zbieranie informacji inwentaryzacyjnych dotyczących sprzętu i oprogramowania z wielu platform.
- Przygotowywanie pakietu aplikacji i przeprowadzanie analizy wpływu poprzedzającej dystrybucję.
- Rozmieszczanie oraz utrzymywanie oprogramowania i zawartości zgodnie z zasadami na pojedynczych komputerach typu desktop, w grupach roboczych lub całych populacjach komputerów typu desktop.
- Zaopatrywanie systemów operacyjnych, aplikacji i zawartości oraz zarządzanie nimi na rozproszonych komputerach typu desktop z dowolnej lokalizacji.
- Integrowanie z produktem HP OpenView Service Desk i innymi narzędziami punktu pomocy i zarządzania systemem.

- Wykorzystywanie wspólnej infrastruktury do zarządzania oprogramowaniem i zawartością na niemal dowolnym urządzeniu, dowolnej platformie i dowolnej sieci dla wszystkich użytkowników korporacyjnych.
- Skalowanie w celu sprostania potrzebom przedsiębiorstwa.

Oprogramowanie HP OpenView Management Suite for Desktops using Radia jest oferowane jako autonomiczne rozwiązanie i jest też w pełni zintegrowane z innymi produktami HP OpenView Management Suite using Radia jako zasadniczy składnik unikalnego podejścia firmy HP opartego na zarządzaniu pożądanym stanem, co zapewnia zautomatyzowane i bieżące utrzymywanie całego oprogramowania zainstalowanego na komputerach w przedsiębiorstwie. Produkty HP OpenView Management Suite using Radia zapewniają, że cała infrastruktura oprogramowania jest zawsze w pożądanym stanie — aktualna, niezawodna i bezpieczna.

Więcej informacji o oprogramowaniu HP OpenView Management Suite for Desktops using Radia można znaleźć na stronie [http://managementsoftware.hp.com/products/radia\\_mdsk/index.html](http://managementsoftware.hp.com/products/radia_mdsk/index.html).

## HP Local Recovery

Oprogramowanie Local Recovery zapewnia ochronę danych i plików systemowych dla komputerów HP Business typu desktop, przenośnych i stacji roboczych. Za pomocą programu Local Recovery można szybko powrócić do pracy w sytuacji przypadkowego usunięcia informacji lub uszkodzenia systemu operacyjnego. Przeznaczone dla użytkowników bez połączenia z siecią lub łączących się rzadko, oprogramowanie Local Recovery chroni dane komputera HP oraz stan systemu za pomocą wykonywanych zgodnie z harmonogramem migawek przechowywanych w chronionym obszarze na lokalnym dysku twardym. Tworzenie kopii zapasowych lub przywracanie można zainicjować przez zwykłe kliknięcie myszą lub naciśnięcie klawisza F1 w środowisku przedrozruchowym. Zadania tworzenia kopii zapasowych systemu i odzyskiwania go po awarii są teraz łatwe dla wszystkich użytkowników, niezależnie od połączenia.

Oprogramowanie Local Recovery jest dostępne bezpłatnie z komputerami HP Business PC. Dostępne są też dwa dodatkowe produkty odzyskiwania komputerów klienckich. Przeprowadzenie uaktualnienia do tych produktów zapewnia dodatkowe funkcje odzyskiwania:

- **Local Recovery Pro** — zawiera wszystkie funkcje oprogramowania Local Recovery i dodatkowo obsługę tworzenia kopii zapasowych i odzyskiwania na pomocniczy dysk twardy oraz zarówno otwartych, jak i zablokowanych plików. Podczas tworzenia migawki kopii zapasowej obsługa otwartych/zablokowanych plików zachowuje informacje w otwartych aplikacjach, takie jak wiadomości e-mail, prezentacje i dokumenty edytorów tekstów.
- **Recovery Solution** — zapewnia pełne rozwiązanie do tworzenia kopii zapasowych i odzyskiwania komputerów na poziomie przedsiębiorstwa z centralnej konsoli administracyjnej. Rozwiązanie obsługuje tworzenie kopii zapasowych danych w chronionym obszarze na lokalnym dysku twardym, jak również w sieciowym obszarze pamięci masowej. Funkcja odzyskiwania oparta na sieci zapewnia wysoki poziom ochrony przed utratą danych spowodowaną awarią dysku twardego bądź kradzieżą lub zagubieniem komputerów.

Więcej informacji o oprogramowaniu HP Local Recovery można znaleźć na stronie [www.hp.com/go/easydeploy](http://www.hp.com/go/easydeploy).

## Dantz Retrospect Express

Oprogramowanie Dantz Retrospect Express chroni pojedynczy komputer typu desktop lub przenośny z systemem Windows. Umożliwia ono odzyskiwanie danych utraconych z powodu wirusów, nowo zainstalowanego oprogramowania, błędów użytkownika, uszkodzeń sprzętu, rozbudowy sprzętu, hakerów oraz utraty czy kradzieży komputerów. Oferuje ono wybór między zwykłymi duplikatami a obszernymi kopiami zapasowymi i jest wyposażone w intuicyjny kreator instalacji, dzięki któremu można przystąpić do używania programu w ciągu kilku minut. Oprogramowanie Retrospect Express jest dostarczane z wbudowaną w produkcie funkcją odzyskiwania po awarii (Disaster Recovery), która zapewnia najlepszą możliwą ochronę. [Kliknij tutaj](#), aby wyświetlić listę producentów sprzętu, którzy dołączają oprogramowanie Retrospect do swoich produktów oraz dowiedzieć się, gdzie można kupić te produkty.

Czas instalacji oprogramowania Retrospect Express i wykonania pierwszej kopii zapasowej nie przekracza dwóch minut. Za pomocą oprogramowania Retrospect można zaimplementować plan tworzenia kopii zapasowych przez udzielenie odpowiedzi na kilka prostych pytań. Proces przywracania przebiega szybko i bezproblemowo. Gdy zajdzie konieczność przywrócenia danych, oprogramowanie Retrospect Express automatycznie odnajduje potrzebne pliki, nawet jeśli użytkownik nie wie, na którym nośniku się znajdują.

Duplikację plików i folderów na zewnętrzny dysk twardy można przeprowadzić przez naciśnięcie jednego przycisku. W trakcie tej operacji informacje są kopiowane z dysku twardego komputera na zewnętrzny dysk twardy. W przypadku zewnętrznych dysków twardych wyposażonych we wbudowany przycisk do tworzenia kopii zapasowych proces duplikowania może zostać zainicjowany przez zwykłe naciśnięcie tego przycisku. Duplikaty plików i folderów przechowywane na zewnętrznym dysku twardym mogą być łatwo przeglądane, obsługiwane i przywracane za pomocą Eksploratora Windows. Proces duplikacji powoduje oszczędność miejsca, przez zastąpienie poprzedniej kopii zapasowej danych na zewnętrznym dysku twardym, oraz oszczędność czasu, przez kopiowanie tylko tych plików, które są nowe lub uległy zmianie od czasu utworzenia ostatniej kopii zapasowej.



Możliwe jest tworzenie kopii zapasowych wielu wersji plików i folderów. Obszerne kopie zapasowe zachowują poprzednie wersje plików oraz folderów i umożliwiają przywrócenie komputera do dowolnego wcześniejszego momentu, zanim nastąpiło uszkodzenie danych. Przy każdym tworzeniu kopii zapasowej oprogramowanie Retrospect Express tworzy punkt przywracania, który może zawierać wszystkie informacje potrzebne użytkownikowi do wczytania pojedynczych plików lub przywrócenia całego komputera (przeprowadzenia odzyskiwania po awarii) — w tym wszystkie pliki i ustawienia systemu operacyjnego, sterowniki urządzeń oraz aplikacje i ich ustawienia. Punkty przywracania są przechwytywane szybko i zapewniają 100% dokładność przywracania do dowolnego momentu, w którym wykonano kopię zapasową, co znacznie wykracza poza możliwości oferowane przez inne programy do tworzenia kopii zapasowych.

Więcej informacji o oprogramowaniu Dantz Retrospect Express można znaleźć na stronie

[http://www.dantz.com/en/products/win\\_express/index.dtml](http://www.dantz.com/en/products/win_express/index.dtml).

## Proactive Change Notification

Program Proactive Change Notification używa witryny sieci Web Subscriber's Choice w celu proaktywnego i automatycznego wykonywania następujących zadań:

- Wysyłanie pocztą e-mail proaktywnych powiadomień o zmianach (Proactive Change Notification — PCN), które z nawet 60-dniowym wyprzedzeniem informują o zmianach w sprzęcie i oprogramowaniu dla większości komercyjnych komputerów i serwerów.
- Wysyłanie wiadomości e-mail zawierających biuletyny, porady dla klientów, ważne informacje, biuletyny dotyczące zabezpieczeń oraz alerty sterowników dla większości komercyjnych komputerów i serwerów.

Użytkownik tworzy swój własny profil w celu zapewnienia sobie otrzymywania tylko informacji związanych z określonym środowiskiem informatycznym. Aby uzyskać więcej informacji o programie Proactive Change Notification i utworzyć profil niestandardowy, należy odwiedzić stronę

<http://h30046.www3.hp.com/subhub.php?jumpid=go/pcn>.

## Subscriber's Choice

Subscriber's Choice to usługa kliencka firmy HP. W oparciu o profil użytkownika firma HP dostarcza mu spersonalizowane porady dotyczące produktów, polecane artykuły i/lub alerty/powiadomienia dotyczące sterowników i wsparcia technicznego. Funkcja alertów/powiadomień dotyczących sterowników i wsparcia usługi Subscriber's Choice dostarcza wiadomości e-mail z powiadomieniem, że informacje zasubskrybowane w profilu są dostępne do przejrzania i pobrania. Aby uzyskać więcej informacji o rozwiązaniu Subscriber's Choice i utworzyć profil niestandardowy, należy odwiedzić stronę: <http://h30046.www3.hp.com/subhub.php>.

## Wycofane rozwiązania

Grupa Desktop Management Task Force (DMTF) wprowadziła standard Desktop Management Interface (DMI) niemal dziesięć lat temu. Ze względu na przyjęcie nowych standardów, takich jak model wspólnych informacji (Common Information Model – CIM), grupa DMTF zainicjowała koniec życia interfejsu DMI. Przy udostępnieniu innych postępowych elementów w oprogramowaniu HP Client Management Solutions, HP Systems Insight Manager i implementacji modelu wspólnych informacji (CMI) firmy Microsoft, znanej pod nazwą Instrumentacja zarządzania Windows (WMI), oprogramowanie HP Insight Management Agent nie jest już udostępniane na nowych komercyjnych komputerach HP typu desktop, stacjach roboczych i przenośnych wprowadzonych po 1 stycznia 2004 r.

Oprogramowanie Insight Management (IM) Agent zapewniało następujące funkcje:

- Obsługa interfejsu DMI umożliwiała zarządzanie systemem klienckim za pomocą programu Insight Manager 7 lub innych aplikacji do zarządzania zgodnych z interfejsem DMI.
- Agent sieci Web umożliwiał zarządzanie systemem zarówno lokalnie, jak i zdalnie za pomocą przeglądarki sieci Web.
- Alerty o stanie mogły powiadamiać użytkownika lokalnie lub być wysyłane do centralnej konsoli.

Program Insight Manager został zastąpiony przez oprogramowanie HP Systems Insight Manager Software (HP SIM). Oprogramowanie HP SIM używa interfejsu WMI do pobierania informacji z systemu klienckiego. Dostępne jest oprogramowanie Altiris Connector for HP Systems Insight Manager, które umożliwia obsługę rozwiązań HP Client Management Solutions za pomocą konsoli HP SIM.

Mimo że alertowanie lokalne nie jest obecnie obsługiwane przez system HP Client Management Solutions, alerty o stanie są przekazywane do konsoli zarządzania systemem. Microsoft WMI jest standardem w systemach Windows 2000 i Windows XP. Instrumentacja WMI zapewnia inwentaryzację sprzętu i informacje o alertach bezpośrednio poprzez system operacyjny Windows do aplikacji zarządzania systemem.

## Pamięć ROM typu flash

System BIOS komputera jest przechowywany w programowalnej pamięci ROM (read only memory) typu flash. W celu zabezpieczenia jej przed nieumyślnym zaktualizowaniem lub zastąpieniem można ustawić hasło konfiguracyjne w programie Computer Setup (F10). Zapewni to operacyjną integralność komputera. Jeżeli zajdzie potrzeba uaktualnienia systemu BIOS, można pobrać najnowsze obrazy BIOS ze strony sterowników i wsparcia technicznego HP (<http://www.hp.com/support/files>).



**PRZESTROGA:** Aby zapewnić maksymalną ochronę pamięci ROM, trzeba pamiętać o ustawieniu hasła konfiguracyjnego. Hasło konfiguracyjne zapobiega nieautoryzowanym uaktualnieniom pamięci ROM. Za pomocą programu System Software Manager administrator systemu może jednocześnie ustawić takie hasło na jednym lub kilku komputerach pracujących w sieci. Więcej informacji można znaleźć na stronie:  
<http://www.hp.com/go/ssm>.

## Zdalne zarządzanie pamięcią ROM typu flash

Funkcja zdalnego zarządzania pamięcią ROM typu flash umożliwia administratorowi systemu zdalne uaktualnianie systemu BIOS komputerów HP pracujących w sieci z jednej centralnej konsoli administracyjnej. Dzięki niej wprowadzane zmiany są identyczne na wszystkich komputerach, a administrator ma większą kontrolę nad procesem uaktualniania obrazów BIOS na sieciowych komputerach firmy HP. W rezultacie ulega poprawie wydajność pracy oraz obniżają się ogólne koszty związane z eksploatacją sieci w przedsiębiorstwie.



Aby możliwe było skorzystanie z funkcji zdalnego zarządzania pamięcią ROM typu flash, komputer musi zostać włączony ręcznie lub zdalnie za pomocą funkcji zdalnego przywracania ze stanu wstrzymania (Remote Wakeup).

Więcej informacji o zdalnym zarządzaniu pamięcią ROM typu flash można znaleźć w części poświęconej oprogramowaniu HP Client Manager Software lub System Software Manager na stronie <http://h18000.www1.hp.com/im/prodinfo.html>.

## HPQFlash

Program narzędziowy HPQFlash służy do lokalnego aktualizowania lub przywracania systemu BIOS na pojedynczych komputerach z poziomu systemu operacyjnego Windows.

Aby uzyskać więcej informacji o narzędziu HPQFlash, należy odwiedzić stronę <http://www.hp.com/support/files> i po wyświetleniu monitu wprowadzić numer modelu komputera.

## Tryb awaryjnego odzyskiwania bloku rozruchowego

Tryb awaryjnego odzyskiwania bloku rozruchowego umożliwia odzyskanie systemu w mało prawdopodobnym przypadku nieudanej aktualizacji pamięci ROM typu flash. Na przykład jeśli podczas uaktualniania systemu BIOS wystąpi awaria zasilania, proces aktualizacji pamięci ROM może zostać niedokończony. W wyniku tego system BIOS może stać się bezużyteczny. Blok rozruchowy stanowi część pamięci ROM, jest jednak zabezpieczony przed aktualizacją. Zawiera on kod, który sprawdza poprawność obrazu systemu BIOS po włączeniu zasilania systemu.

- Jeżeli sprawdzenie poprawności przebiegnie pomyślnie, system zostanie uruchomiony w zwykły sposób.
- Jeśli system BIOS jest niepoprawny, system BIOS w bezpiecznym bloku rozruchowym umożliwi:
  - ❑ przeszukanie nośników wymiennych pod kątem plików obrazów systemu BIOS; po odnalezieniu właściwego pliku obrazu systemu BIOS zostanie on automatycznie wczytany do pamięci ROM.
  - ❑ uruchomienie systemu z rozruchowego nośnika wymiennego, który automatycznie uruchomi narzędzia uaktualniania systemu BIOS.

Po wykryciu nieprawidłowego obrazu systemu BIOS dioda zasilania zamiga w kolorze czerwonym 8 razy w jednosekundowych odstępach. Jednocześnie głośnik wyemituje 8 sygnałów dźwiękowych. Jeśli część systemowej pamięci ROM zawierająca obraz opcjonalnej pamięci ROM wideo nie jest uszkodzona, na ekranie zostanie wyświetlony komunikat Boot Block Emergency Recovery Mode.

Aby odzyskać system po uruchomieniu go w trybie awaryjnego odzyskiwania bloku rozruchowego:

1. Wyłącz zasilanie.
2. Włóż dyskietkę, dysk CD lub urządzenie USB typu flash zawierające żądany plik obrazu systemu BIOS w katalogu głównym. Uwaga: Nośnik musi być sformatowany przy użyciu systemu plików FAT12, FAT16 lub FAT32.
3. Włącz komputer.

Jeśli nie zostanie odnaleziony właściwy plik obrazu systemu BIOS, system BIOS w bezpiecznym bloku rozruchowym podejmie próbę uruchomienia systemu z urządzenia rozruchowego. Jeśli nie zostanie odnalezione urządzenie rozruchowe, pojawi się monit o włożenie nośnika zawierającego plik obrazu systemu BIOS lub narzędzie uaktualniania systemu BIOS.

Jeśli system pomyślnie przeprogramuje pamięć ROM, nastąpi automatyczne wyłączenie zasilania systemu.

4. Wyjmij nośnik wymienny użyty do uaktualnienia systemu BIOS.
5. Włącz zasilanie, aby uruchomić ponownie komputer.

## Replikowanie ustawień konfiguracyjnych

Przy użyciu poniższych procedur administrator może w prosty sposób kopiować ustawienia konfiguracyjne z jednego komputera na inne (ten sam model). Umożliwia to zachowanie zgodności danych konfiguracyjnych na wielu komputerach.



W przypadku obu procedur wymagany jest napęd dyskietek lub obsługiwane urządzenie USB typu flash, np. HP Drive Key.

---

## Kopiowanie na jeden komputer



**PRZESTROGA:** Ustawienia konfiguracyjne są specyficzne dla modelu komputera. Jeśli modele komputera źródłowego i docelowego są różne, może dojść do uszkodzenia systemu plików. Przykładowo nie należy kopiować ustawień konfiguracyjnych z komputera dc7xxx na komputer dx7xxx.

---

1. Wybierz ustawienia konfiguracyjne do skopiowania. Wyłącz komputer. W systemie Windows kliknij kolejno **Start > Zamknij > Zamknij system**.
  2. Jeżeli używane jest urządzenie USB typu flash, podłącz je teraz.
  3. Włącz komputer.
  4. Zaraz po włączeniu komputera, gdy dioda zasilania monitora zaświeci się na zielono, naciśnij klawisz **F10**, aby otworzyć program Computer Setup. W razie potrzeby możesz nacisnąć klawisz **Enter**, aby pominąć ekran tytułowy.
- 



Jeśli klawisz **F10** nie zostanie naciśnięty w odpowiednim czasie, dostęp do programu będzie możliwy dopiero po ponownym uruchomieniu komputera, a następnie ponownym naciśnięciu klawisza **F10**, gdy dioda zasilania monitora zaświeci się na zielono.

---

5. Jeżeli używana jest dyskietka, włóż ją teraz.

6. Kliknij kolejno **File (Plik) > Replicated Setup (Zreplikowane ustawienia) > Save to Removable Media (Zapisz na nośniku wymiennym)**. Postępuj zgodnie z instrukcjami pojawiającymi się na ekranie, aby zapisać ustawienia konfiguracyjne na dyskiecie lub w urządzeniu USB typu flash.
7. Wyłącz komputer, który ma zostać skonfigurowany, a następnie włóż dyskietkę konfiguracyjną do napędu lub podłącz urządzenie USB typu flash.
8. Włącz komputer.
9. Zaraz po włączeniu komputera, gdy dioda zasilania monitora zaświeci się na zielono, naciśnij klawisz **F10**, aby otworzyć program Computer Setup. W razie potrzeby możesz nacisnąć klawisz **Enter**, aby pominąć ekran tytułowy.
10. Kliknij kolejno **File (Plik) > Replicated Setup (Zreplikowane ustawienia) > Restore from Removable Media (Przywróć z nośnika wymiennego)**, a następnie postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.
11. Po ukończeniu konfiguracji uruchom ponownie komputer.

## Kopiowanie na wiele komputerów



**PRZESTROGA:** Ustawienia konfiguracyjne są specyficzne dla modelu komputera. Jeśli modele komputera źródłowego i docelowego są różne, może dojść do uszkodzenia systemu plików. Przykładowo nie należy kopiować ustawień konfiguracyjnych z komputera dc7xxx na komputer dx7xxx.

Wprowadzanie przygotowanej dyskietki konfiguracyjnej lub urządzenia USB typu flash przy użyciu tej metody trwa nieznacznie dłużej, ale dane są kopiowane na komputery docelowe znacznie szybciej.



Do wykonania tej procedury lub utworzenia rozruchowego urządzenia USB typu flash wymagana jest dyskietka rozruchowa. Jeśli nie jest dostępny komputer z systemem umożliwiającym utworzenie dyskietki rozruchowej (Windows XP), należy skorzystać z metody kopiowania na jeden komputer (zobacz część „[Kopiowanie na jeden komputer](#)” na stronie 18).

1. Utwórz dyskietkę rozruchową lub rozruchowe urządzenie USB typu flash. Informacje można znaleźć w części „Obsługiwane urządzenie USB typu flash“ na stronie 21 lub „Nieobsługiwane urządzenie USB typu flash“ na stronie 24.



**PRZESTROGA:** Nie wszystkie komputery można uruchomić za pomocą urządzenia USB typu flash. Jeśli urządzenie USB jest wymienione przed dyskiem twardym na liście domyślnej kolejności rozruchu urządzeń w programie Computer Setup (F10), taki komputer można uruchomić za pomocą urządzenia USB typu flash. W innym przypadku należy użyć dyskietki rozruchowej.

2. Wybierz ustawienia konfiguracyjne do skopiowania. Wyłącz komputer. W systemie Windows kliknij kolejno **Start > Zamknij > Zamknij system**.
3. Jeżeli używane jest urządzenie USB typu flash, podłącz je teraz.
4. Włącz komputer.
5. Zaraz po włączeniu komputera, gdy dioda zasilania monitora zaświeci się na zielono, naciśnij klawisz **F10**, aby otworzyć program Computer Setup. W razie potrzeby możesz nacisnąć klawisz **Enter**, aby pominąć ekran tytułowy.



Jeśli klawisz **F10** nie zostanie naciśnięty w odpowiednim czasie, dostęp do programu będzie możliwy dopiero po ponownym uruchomieniu komputera, a następnie ponownym naciśnięciu klawisza **F10**, gdy dioda zasilania monitora zaświeci się na zielono.

6. Jeżeli używana jest dyskietka, włóż ją teraz.
7. Kliknij kolejno **File (Plik) > Replicated Setup (Zreplikowane ustawienia) > Save to Removable Media (Zapisz na nośniku wymiennym)**. Postępuj zgodnie z instrukcjami pojawiającymi się na ekranie, aby zapisać ustawienia konfiguracyjne na dyskietce lub w urządzeniu USB typu flash.
8. Pobierz program narzędziowy BIOS służący do replikowania ustawień konfiguracyjnych (repset.exe) i skopiuj go na dyskietkę konfiguracyjną lub konfiguracyjne urządzenie USB typu flash. Aby pobrać ten program, wejdź na stronę [tap://welcome.hp.com/support/files](http://welcome.hp.com/support/files) i wprowadź numer modelu komputera.



9. Na dyskietce konfiguracyjnej lub w konfiguracyjnym urządzeniu USB typu flash utwórz plik autoexec.bat zawierający następujące polecenie:

**reset.exe**

10. Wyłącz komputer, który ma zostać skonfigurowany. Włóż dyskietkę konfiguracyjną lub konfiguracyjne urządzenie USB typu flash, a następnie włącz komputer. Program konfiguracyjny zostanie uruchomiony automatycznie.
11. Po ukończeniu konfiguracji uruchom ponownie komputer.

## Tworzenie urządzenia rozruchowego

### Obsługiwane urządzenie USB typu flash

Obsługiwane urządzenia są wyposażone w preinstalowany obraz, co upraszcza proces przekształcania ich w urządzenia rozruchowe. W obraz taki są wyposażone wszystkie urządzenia USB typu flash firmy HP lub Compaq i większość urządzeń tego typu innych firm. Jeśli używane urządzenie USB typu flash nie jest wyposażone w taki obraz, należy użyć procedury opisanej dalej w tej części (zobacz [„Nieobsługiwane urządzenie USB typu flash“ na stronie 24](#)).

Do utworzenia rozruchowego urządzenia USB typu flash wymagane są następujące elementy:

- Obsługiwane urządzenie USB typu flash.
- Rozruchowa dyskietka DOS zawierająca programy FDISK i SYS. (Jeśli program SYS jest niedostępny, można użyć programu FORMAT, lecz spowoduje to utratę wszystkich plików zapisanych już w urządzeniu USB typu flash).
- Komputer PC, którego rozruch można przeprowadzić z urządzenia USB typu flash.



**PRZESTROGA:** W przypadku niektórych starszych komputerów PC rozruch z urządzenia USB typu flash może być niemożliwy. Jeśli urządzenie USB jest wymienione przed dyskiem twardym na liście domyślnej kolejności rozruchu urządzeń w programie Computer Setup (F10), taki komputer można uruchomić za pomocą urządzenia USB typu flash. W innym przypadku należy użyć dyskietki rozruchowej.

1. Wyłącz komputer.
2. Podłącz urządzenie USB typu flash do jednego z portów USB komputera i odłącz wszystkie inne urządzenia pamięci masowej USB (oprócz napędów dyskietek USB).
3. Włóż do napędu dyskietkę rozruchową DOS z programem FDISK.COM oraz programem SYS.COM lub FORMAT.COM. Następnie włącz komputer, aby przeprowadzić jego rozruch z dyskietki DOS.
4. Uruchom program FDISK z wiersza A:\, wpisując **FDISK** i naciskając klawisz Enter. Po wyświetleniu monitu kliknij przycisk **Yes (Y)**, aby włączyć obsługę napędów o dużej pojemności.
5. Wprowadź numer [**5**], aby wyświetlić listę napędów w systemie. Urządzenie USB typu flash można zidentyfikować po rozmiarze dysku. Odpowiada mu napęd, którego rozmiar jest najbardziej zbliżony — zazwyczaj ostatni napęd z listy. Zanotuj literę napędu.

Napęd urządzenia USB typu flash: \_\_\_\_\_



**PRZESTROGA:** Jeśli ten napęd nie odpowiada urządzeniu USB typu flash, nie należy kontynuować procedury. Może to spowodować utratę danych. Należy sprawdzić wszystkie porty USB pod kątem innych urządzeń pamięci masowej. W przypadku ich znalezienia należy odłączyć te urządzenia, a następnie uruchomić ponownie komputer i kontynuować procedurę od punktu 4. Jeśli takie urządzenia nie zostaną znalezione, może to oznaczać, że system nie obsługuje urządzeń USB typu flash lub podłączone urządzenie USB typu flash jest uszkodzone. **NIE** należy kontynuować procedury przekształcania urządzenia USB typu flash w urządzenie rozruchowe.

---

6. Wyjdź z programu FDISK, naciskając klawisz **Esc** w celu powrotu do wiersza A:\.
7. Jeśli dyskietka rozruchowa DOS zawiera program SYS.COM, przejdź do punktu 8. W przeciwnym razie przejdź do punktu 9.
8. W wierszu A:\ wprowadź polecenie **SYS x:**, gdzie x oznacza zanotowaną wcześniej literę napędu.



**PRZESTROGA:** Należy pamiętać o wprowadzeniu poprawnej litery napędu dla urządzenia USB typu flash.

---

Po przetransferowaniu plików systemowych program SYS powróci do wiersza A:\. Przejdź do punktu 13.

9. Wybierz pliki, które chcesz zachować, i skopiuj je z urządzenia USB typu flash do katalogu tymczasowego na innym dysku (np. wewnętrznym dysku twardym systemu).
  10. W wierszu A:\ wprowadź polecenie **FORMAT /S X:**, gdzie X oznacza zanotowaną wcześniej literę napędu.
- 



**PRZESTROGA:** Należy pamiętać o wprowadzeniu poprawnej litery napędu dla urządzenia USB typu flash.

---

Polecenie FORMAT spowoduje wyświetlenie jednego lub większej liczby ostrzeżeń i za każdym razem pojawi się pytanie, czy proces ma być kontynuowany. W odpowiedzi należy każdorazowo wpisać literę **Y**. Polecenie FORMAT spowoduje sformatowanie urządzenia USB typu flash i dodanie plików systemowych. Zostanie również wyświetlone zapytanie o etykietę woluminu.

11. Wprowadź etykietę (jeśli jest potrzebna) lub naciśnij klawisz **Enter**, aby ją pominąć.
  12. Skopiuj wszystkie pliki zapisane w punkcie 9 na urządzenie USB typu flash.
  13. Wyjmij dyskietkę i uruchom ponownie komputer. Komputer zostanie uruchomiony z urządzeniem USB typu flash jako dyskiem C.
- 



Na każdym komputerze może być określona inna domyślna kolejność rozruchu urządzeń — do jej zmiany służy program narzędziowy Computer Setup (F10).

W wersji DOS dla środowiska Windows 9x może się chwilowo pojawić ekran z logo systemu Windows. Jeśli ten ekran nie ma być wyświetlany, w katalogu głównym urządzenia USB typu flash należy dodać plik o rozmiarze zerowym i nazwie LOGO.SYS.

---

Powrót do „[Kopiowanie na wiele komputerów](#)“ na stronie 19.

## Nieobsługiwane urządzenie USB typu flash

Do utworzenia rozruchowego urządzenia USB typu flash wymagane są następujące elementy:

- Urządzenie USB typu flash.
- Rozruchowa dyskietka DOS zawierająca programy FDISK i SYS. (Jeśli program SYS jest niedostępny, można użyć programu FORMAT, lecz spowoduje to utratę wszystkich plików zapisanych już w urządzeniu USB typu flash).
- Komputer PC, którego rozruch można przeprowadzić z urządzenia USB typu flash.



---

**PRZESTROGA:** W przypadku niektórych starszych komputerów PC rozruch z urządzenia USB typu flash może być niemożliwy. Jeśli urządzenie USB jest wymienione przed dyskiem twardym na liście domyślnej kolejności rozruchu urządzeń w programie Computer Setup (F10), taki komputer można uruchomić za pomocą urządzenia USB typu flash. W innym przypadku należy użyć dyskietki rozruchowej.

---

1. Jeśli w systemie znajdują się karty PCI z dołączonymi napędami SCSI, ATA RAID lub SATA, wyłącz komputer i odłącz kabel zasilający.



---

**PRZESTROGA:** Kabel zasilający MUSI zostać odłączony.

---

2. Zdejmij pokrywę komputera i wyjmij karty PCI.
3. Podłącz urządzenie USB typu flash do jednego z portów USB komputera i odłącz wszystkie inne urządzenia pamięci masowej USB (oprócz napędów dyskietek USB). Zamknij pokrywę komputera.
4. Podłącz kabel zasilający i włącz komputer.
5. Zaraz po włączeniu komputera, gdy dioda zasilania monitora zaświeci się na zielono, naciśnij klawisz **F10**, aby otworzyć program Computer Setup. W razie potrzeby możesz nacisnąć klawisz **Enter**, aby pominąć ekran tytułowy.



Jeśli klawisz **F10** nie zostanie naciśnięty w odpowiednim czasie, dostęp do programu będzie możliwy dopiero po ponownym uruchomieniu komputera, a następnie ponownym naciśnięciu klawisza **F10**, gdy dioda zasilania monitora zaświeci się na zielono.

6. Wybierz kolejno **Advanced (Zaawansowane) > PCI Devices (Urządzenia PCI)**, aby wyłączyć kontrolery PATA i SATA. Wyłączając kontroler SATA należy zanotować przerwanie IRQ, do którego jest on przypisany. Informacja ta będzie później potrzebna do ponownego przypisania przerwania IRQ. Zamknij program konfiguracyjny i potwierdź zmiany.  
Przerwanie IRQ SATA: \_\_\_\_\_
7. Włóż do napędu dyskietkę rozruchową DOS z programem FDISK.COM oraz programem SYS.COM lub FORMAT.COM. Następnie włącz komputer, aby uruchomić go z dyskietki DOS.
8. Uruchom program FDISK i usuń wszystkie istniejące partycje urządzenia USB typu flash. Utwórz nową partycję i oznacz ją jako aktywną. Zamknij program FDISK, naciskając klawisz **Esc**.
9. Jeśli po zamknięciu programu FDISK system nie zostanie automatycznie ponownie uruchomiony, naciśnij kombinację klawiszy **Ctrl+Alt+Del**, aby ponownie uruchomić system z dyskietki DOS.
10. W wierszu A:\ wprowadź polecenie **FORMAT C: /S**, a następnie naciśnij klawisz **Enter**. Spowoduje to sformatowanie urządzenia USB typu flash i dodanie plików systemowych. Zostanie również wyświetlone zapytanie o etykietę woluminu.
11. Wprowadź etykietę (jeśli jest potrzebna) lub naciśnij klawisz **Enter**, aby ją pominąć.
12. Wyłącz komputer i odłącz kabel zasilający. Otwórz pokrywę komputera i ponownie zainstaluj wszystkie wyjęte wcześniej karty PCI. Zamknij pokrywę komputera.
13. Podłącz kabel zasilający, wyjmij z napędu dyskietkę, a następnie włącz komputer.

14. Zaraz po włączeniu komputera, gdy dioda zasilania monitora zaświeci się na zielono, naciśnij klawisz **F10**, aby otworzyć program Computer Setup. W razie potrzeby możesz nacisnąć klawisz **Enter**, aby pominąć ekran tytułowy.
15. Wybierz kolejno **Advanced (Zaawansowane) > PCI devices (Urządzenia PCI)** i ponownie włącz kontrolery PATA i SATA, które zostały wyłączone w punkcie 6. Przypisz kontroler SATA do jego pierwotnego przerwania IRQ.
16. Zapisz zmiany i zakończ pracę programu. Komputer zostanie uruchomiony z urządzeniem USB typu flash jako dyskiem C.



---

Na każdym komputerze może być określona inna domyślna kolejność rozruchu urządzeń — do jej zmiany służy program narzędziowy Computer Setup (F10). Więcej informacji na ten temat można znaleźć w *Podręczniku do programu Computer Setup* na dysku CD *Dokumentacja i diagnostyka*.

W wersji DOS dla środowiska Windows 9x może się chwilowo pojawić ekran z logo systemu Windows. Jeśli ten ekran nie ma być wyświetlany, w katalogu głównym urządzenia USB typu flash należy dodać plik o rozmiarze zerowym i nazwie LOGO.SYS.

---

Powrót do „[Kopiowanie na wiele komputerów](#)“ na stronie 19.

## Dwufunkcyjny przycisk zasilania

Jeżeli aktywny jest interfejs zaawansowanego zarządzania konfiguracją i zasilaniem (ACPI), przycisk zasilania komputera może działać jako włącznik/wyłącznik zasilania lub jako przycisk wstrzymania. Działanie funkcji wstrzymania polega na tym, że komputer nie jest zupełnie wyłączany, ale wprowadzany w stan niskiego poboru energii. Pozwala to na szybkie zmniejszenie zużycia energii (przejście do trybu oszczędzania energii) bez konieczności zamykania programów, a także szybki powrót do tego samego stanu bez ryzyka utraty danych.

Aby zmienić sposób działania przycisku zasilania, wykonaj następujące czynności:

1. Kliknij przycisk **Start**, a następnie wybierz kolejno **Panel sterowania > Opcje zasilania**.
2. W oknie **Właściwości: Opcje zasilania** wybierz kartę **Zaawansowane**.
3. W sekcji **Przycisk zasilania** wybierz opcję **Stan wstrzymania**.

Po skonfigurowaniu przycisku zasilania jako przycisku wstrzymania jego naciśnięcie spowoduje przejście systemu w stan niskiego poboru energii (stan wstrzymania). Ponowne jego naciśnięcie spowoduje natomiast szybkie uaktywnienie systemu i przejście komputera do trybu pełnego zasilania. Aby całkowicie wyłączyć komputer, należy nacisnąć przycisk zasilania i przytrzymać go w tej pozycji przez kilka sekund.



**PRZESTROGA:** Przycisku zasilania należy używać do wyłączania komputera tylko w przypadku braku odpowiedzi systemu. Wyłączanie zasilania bez interakcji ze strony systemu operacyjnego może doprowadzić do uszkodzenia lub utraty danych zgromadzonych na dysku twardym.

---

## Witryna sieci Web

Personel techniczny firmy HP na bieżąco testuje i usuwa błędy w programach własnych oraz dostarczanych przez innych producentów, jak również prowadzi prace nad oprogramowaniem wspomagającym, przeznaczonym dla różnych systemów operacyjnych. Zapewnia to wydajność, zgodność i niezawodność komputerów firmy HP.

Wskazane jest, aby podczas zmiany lub uaktualniania systemów operacyjnych zaimplementować zaprojektowane dla nich oprogramowanie wspomagające. Jeśli planowane jest korzystanie z wersji systemu Microsoft Windows innej niż zainstalowana fabrycznie, należy zainstalować odpowiednie sterowniki urządzeń oraz programy narzędziowe (dzięki temu wszystkie dostępne funkcje będą realizowane poprawnie).

Dzięki staraniom firmy HP procesy odnajdywania, uzyskiwania dostępu, uaktualniania i instalowania najnowszego oprogramowania wspomagającego są bardzo proste. Oprogramowanie można pobrać ze strony <http://www.hp.com/support>.

W witrynie tej dostępne są najnowsze wersje sterowników urządzeń, programy narzędziowe oraz możliwe do aktualizowania obrazy pamięci ROM, niezbędne do pracy najnowszej wersji systemu Windows na komputerach firmy HP.

## Współpraca z innymi producentami

Opracowane przez firmę HP rozwiązania do zarządzania integrują się z innymi aplikacjami do zarządzania systemem i są oparte na standardach przemysłowych, takich jak:

- Zarządzanie oparte na sieci Web  
(Web-Based Enterprise Management — WBEM)
- Interfejs zarządzania Windows  
(Windows Management Interface — WMI)
- Technologia Wake on LAN
- ACPI
- SMBIOS
- Środowisko Pre-boot Execution (PXE)



## Śledzenie i zabezpieczanie majątku

Komputery firmy HP są wyposażone w funkcje śledzenia majątku. Zgromadzone dane dotyczące stanu kluczowych zasobów mogą być przetwarzane za pomocą oprogramowania HP Systems Insight Manager, HP Client Manager lub innych aplikacji do zarządzania systemem. Ze względu na całkowitą i automatyczną integrację funkcji śledzenia majątku ze wspomnianymi programami, użytkownik może wybrać narzędzie do zarządzania najlepiej odpowiadające jego środowisku pracy oraz podnoszące efektywność już używanego oprogramowania narzędziowego.

Firma HP oferuje również kilka rozwiązań służących do kontroli dostępu do cennych podzespołów i informacji. Oprogramowanie HP Embedded Security for ProtectTools (po zainstalowaniu) zapobiega nieautoryzowanemu dostępowi do danych, a także sprawdza integralność systemu i uwierzytelnia innych użytkowników próbujących uzyskać dostęp do systemu. (Więcej informacji można znaleźć w *Podręczniku oprogramowania HP ProtectTools Security Manager* w witrynie [www.hp.com](http://www.hp.com)). Dostępne w niektórych modelach funkcje zabezpieczeń, takie jak HP Embedded Security for ProtectTools, blokada Smart Cover Lock i czujnik Smart Cover Sensor, zapobiegają nieautoryzowanemu dostępowi do wewnętrznych podzespołów komputera. Z kolei wyłączając porty szeregowo, równoległe lub USB albo wyłączając możliwość rozruchu systemu z nośników wymiennych, można chronić cenne dane. Alerty dotyczące zmiany rozmiaru pamięci oraz otwarcia pokrywy mogą być automatycznie przesyłane do aplikacji zarządzania systemem, przez co będą pełniły funkcję proaktywnego powiadamiania o ingerencji w wewnętrzne elementy komputera.





HP Embedded Security for ProtectTools, czujnik Smart Cover Sensor i blokada Smart Cover Lock są dostępne jako opcje w niektórych systemach.

Ustawienia zabezpieczeń komputerów firmy HP mogą być zarządzane na dwa sposoby:



- Lokalnie, za pomocą oprogramowania narzędziowego Computer Setup. Dodatkowe informacje i instrukcje dotyczące korzystania z programu Computer Setup można znaleźć w *Podręczniku do programu Computer Setup (F10)* na dołączonym do komputera dysku CD *Dokumentacja i diagnostyka*.
- Zdalnie, za pomocą programu HP Client Manager Software lub System Software Manager, umożliwiającego bezpieczne rozmieszczanie i kontrolowanie jednolitych ustawień zabezpieczeń z poziomu prostego narzędzia wiersza polecenia.

Poniższa tabela oraz dalsze części dotyczą lokalnego zarządzania funkcjami zabezpieczeń komputera za pomocą oprogramowania narzędziowego Computer Setup (F10).


## Przegląd funkcji zabezpieczeń

Opcja	Opis
Setup Password (Hasło konfiguracyjne)	<p>Umożliwia ustawianie i włączanie hasła konfiguracyjnego (administratora).</p> <p> Jeżeli ustawione zostanie hasło konfiguracyjne, jego wprowadzanie jest wymagane przy próbie: zmiany opcji programu Computer Setup, zaktualizowania pamięci ROM typu flash i zmiany określonych ustawień plug and play w systemie Windows.</p> <p>Więcej informacji na ten temat można znaleźć w <i>Podręczniku rozwiązywania problemów</i> na dysku CD <i>Dokumentacja i diagnostyka</i>.</p>
Power-On Password (Hasło uruchomieniowe)	<p>Umożliwia ustawianie i włączanie hasła uruchomieniowego.</p> <p>Więcej informacji na ten temat można znaleźć w <i>Podręczniku rozwiązywania problemów</i> na dysku CD <i>Dokumentacja i diagnostyka</i>.</p>
Password Options (Opcje haseł) (Opcja ta zostanie wyświetlona tylko pod warunkiem, że ustawiono hasło uruchomieniowe).	<p>Umożliwia określenie, czy przy ponownym uruchomieniu komputera bez wyłączenia zasilania (za pomocą kombinacji klawiszy <b>CTRL+ALT+DEL</b>) wymagane jest podanie hasła.</p> <p>Więcej informacji na ten temat można znaleźć w <i>Podręczniku do programu Computer Setup (F10)</i> na dysku CD <i>Dokumentacja i diagnostyka</i>.</p>
Pre-Boot Authorization (Autoryzacja przed rozruchem)	<p>Umożliwia włączanie/wyłączanie karty inteligentnej, która może być używana w zastępstwie hasła uruchomieniowego.</p>
 Więcej informacji o programie Computer Setup można znaleźć w <i>Podręczniku do programu Computer Setup (F10)</i> na dysku CD <i>Dokumentacja i diagnostyka</i> .	<p>Obsługa funkcji zabezpieczeń może się różnić w zależności od konfiguracji komputera.</p>



## Przegląd funkcji zabezpieczeń (ciąg dalszy)

Opcja	Opis
Smart Cover	<p>Umożliwia:</p> <ul style="list-style-type: none"> <li>• Włączanie/wyłączanie blokady Smart Cover Lock.</li> <li>• Włączanie/wyłączanie czujnika Cover Removal Sensor.</li> </ul> <p> Funkcja <i>Notify User</i> służy do powiadamiania użytkownika o tym, że pokrywa została zdjęta. Jeśli zostanie wybrana funkcja <i>Setup Password</i>, to aby można było uruchomić komputer ze zdjętą pokrywą, wymagane jest wprowadzenie hasła konfiguracyjnego.</p> <p>Funkcja ta jest obsługiwana jedynie w niektórych modelach. Więcej informacji na ten temat można znaleźć w <i>Podręczniku do programu Computer Setup (F10)</i> na dysku CD <i>Dokumentacja i diagnostyka</i>.</p>
Embedded Security (Wbudowany mikroukład zabezpieczeń)	<p>Umożliwia:</p> <ul style="list-style-type: none"> <li>• Włączanie/wyłączanie urządzenia obsługującego wbudowany mikroukład zabezpieczeń.</li> <li>• Przywracanie fabrycznych ustawień urządzenia.</li> </ul> <p>Funkcja ta jest obsługiwana jedynie w niektórych modelach. Więcej informacji można znaleźć w <i>Podręczniku oprogramowania HP ProtectTools Security Manager</i> w witrynie <a href="http://www.hp.com">www.hp.com</a>.</p>
Device Security (Zabezpieczenia urządzeń)	<p>Włącza/wyłącza porty szeregowy, port równoległy, przednie porty USB, dźwięk systemowy, kontrolery sieci (wybrane modele), urządzenia MultiBay (wybrane modele) oraz kontrolery SCSI (wybrane modele).</p>
<p> Więcej informacji o programie <i>Computer Setup</i> można znaleźć w <i>Podręczniku do programu Computer Setup (F10)</i> na dysku CD <i>Dokumentacja i diagnostyka</i>.</p> <p>Obsługa funkcji zabezpieczeń może się różnić w zależności od konfiguracji komputera.</p>	

## Przegląd funkcji zabezpieczeń (ciąg dalszy)

Opcja	Opis
Network Service Boot (Rozruch z sieci)	Włącza/wyłącza możliwość rozruchu komputera z systemu operacyjnego zainstalowanego na serwerze sieciowym. Funkcja ta jest dostępna tylko w modelach wyposażonych w kontroler interfejsu sieciowego (NIC). Kontroler sieci musi być zainstalowany w magistrali PCI lub bezpośrednio na płycie głównej.
System IDs (Identyfikatory systemowe)	<p>Umożliwia ustawianie następujących opcji:</p> <ul style="list-style-type: none"> <li>Etykiety zasobu (identyfikator składający się z 18 znaków) i etykiety właściciela (identyfikator składający się z 80 znaków i wyświetlany podczas autotestu POST).</li> </ul> <p>Więcej informacji na ten temat można znaleźć w <i>Podręczniku do programu Computer Setup (F10)</i> na dysku CD <i>Dokumentacja i diagnostyka</i>.</p> <ul style="list-style-type: none"> <li>Numeru seryjnego podstawy montażowej lub uniwersalnego unikatowego identyfikatora (UUID). Identyfikator UUID można aktualizować, tylko jeśli bieżący numer seryjny podstawy montażowej jest błędny. (Zazwyczaj numery te są ustawiane fabrycznie i służą za unikatowe identyfikatory systemu).</li> </ul> <p>Układu klawiatury (np. angielska lub niemiecka) do wprowadzania systemowych danych identyfikacyjnych.</p>
<p> Więcej informacji o programie Computer Setup można znaleźć w <i>Podręczniku do programu Computer Setup (F10)</i> na dysku CD <i>Dokumentacja i diagnostyka</i>.</p> <p>Obsługa funkcji zabezpieczeń może się różnić w zależności od konfiguracji komputera.</p>	

## Przegląd funkcji zabezpieczeń (ciąg dalszy)

Opcja	Opis
DriveLock (niektóre modele)	<p>Umożliwia przydzielanie i modyfikowanie hasła głównego lub hasła użytkownika dla dysków twardych ATA. Włączenie tej funkcji spowoduje, że podczas autotestu POST użytkownik będzie monitowany o podanie jednego z haseł DriveLock. Jeśli żadne z nich nie zostanie pomyślnie wprowadzone, dysk twardy chroniony hasłem będzie niedostępny do momentu wprowadzenia poprawnego hasła podczas kolejnego uruchomienia komputera.</p> <p> Opcja ta jest wyświetlana tylko w przypadku, gdy w systemie został zainstalowany co najmniej jeden dysk ATA obsługujący zestaw poleceń ATA Security.</p> <p>Więcej informacji na ten temat można znaleźć w <i>Podręczniku do programu Computer Setup (F10)</i> na dysku CD <i>Dokumentacja i diagnostyka</i>.</p>
<p> Więcej informacji o programie Computer Setup można znaleźć w <i>Podręczniku do programu Computer Setup (F10)</i> na dysku CD <i>Dokumentacja i diagnostyka</i>.</p> <p>Obsługa funkcji zabezpieczeń może się różnić w zależności od konfiguracji komputera.</p>	

## Zabezpieczanie hasłem

Hasło uruchomieniowe zapobiega nieautoryzowanemu dostępowi do komputera. Jego podanie jest wymagane przy każdorazowym włączaniu lub ponownym uruchamianiu komputera. Hasło konfiguracyjne zapobiega nieautoryzowanemu dostępowi do programu Computer Setup. Można go również używać jako hasła uruchomieniowego. Oznacza to, że podanie hasła konfiguracyjnego zamiast uruchomieniowego umożliwi uzyskanie dostępu do zasobów komputera.

Administrator systemu może dysponować hasłem konfiguracyjnym obowiązującym w całej sieci. Dzięki niemu ma on dostęp do wszystkich komputerów oraz możliwość sprawowania kontroli nad działaniem całego systemu, nawet jeżeli stanowiska są chronione za pomocą haseł uruchomieniowych.

## Ustawianie hasła konfiguracyjnego za pomocą programu Computer Setup

Jeśli system jest wyposażony we wbudowany mikroukład zabezpieczeń, należy zapoznać się z informacjami w *Podręczniku oprogramowania HP ProtectTools Security Manager* w witrynie [www.hp.com](http://www.hp.com). Ustawienie hasła konfiguracyjnego za pomocą programu Computer Setup zapobiega przypadkowym i nieautoryzowanym zmianom konfiguracji komputera, gdyż dostęp do programu Computer Setup (F10) będzie możliwy wyłącznie po podaniu tego hasła.

1. Włącz lub uruchom ponownie komputer. W systemie Windows kliknij kolejno **Start > Zamknij > Uruchom ponownie**.
2. Zaraz po włączeniu komputera, gdy dioda zasilania monitora zaświeci się na zielono, naciśnij klawisz **F10**, aby otworzyć program Computer Setup. W razie potrzeby możesz nacisnąć klawisz **Enter**, aby pominąć ekran tytułowy.



Jeśli klawisz **F10** nie zostanie naciśnięty w odpowiednim czasie, dostęp do programu będzie możliwy dopiero po ponownym uruchomieniu komputera, a następnie ponownym naciśnięciu klawisza **F10**, gdy dioda zasilania monitora zaświeci się na zielono.

3. Wybierz menu **Security (Zabezpieczenia)**, wybierz opcję **Setup Password (Hasło konfiguracyjne)**, a następnie postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.
4. Przed wyjściem z programu kliknij kolejno **File (Plik) > Save Changes and Exit (Zapisz zmiany i zakończ)**.

## Ustawianie hasła uruchomieniowego za pomocą programu Computer Setup

Po ustawieniu hasła uruchomieniowego za pomocą programu Computer Setup dostęp do danych komputera jest możliwy dopiero po podaniu poprawnego hasła. Ustawienie tego hasła spowoduje również wyświetlenie w menu Security (Zabezpieczenia) programu Computer Setup pozycji Password Options (Opcje hasła). Do opcji hasła należy Password Prompt on Warm Boot (Wymaganie hasła przy ponownym uruchamianiu bez wyłączania zasilania). Jeżeli włączona zostanie opcja Password Prompt on Warm Boot, wprowadzanie hasła będzie konieczne również przy każdym ponownym uruchomieniu komputera.

1. Włącz lub uruchom ponownie komputer. W systemie Windows kliknij kolejno **Start > Zamknij > Uruchom ponownie**.
2. Zaraz po włączeniu komputera, gdy dioda zasilania monitora zaświeci się na zielono, naciśnij klawisz **F10**, aby otworzyć program Computer Setup. W razie potrzeby możesz nacisnąć klawisz **Enter**, aby pominąć ekran tytułowy.



Jeśli klawisz **F10** nie zostanie naciśnięty w odpowiednim czasie, dostęp do programu będzie możliwy dopiero po ponownym uruchomieniu komputera, a następnie ponownym naciśnięciu klawisza **F10**, gdy dioda zasilania monitora zaświeci się na zielono.

3. Wybierz menu **Security (Zabezpieczenia)**, wybierz opcję **Power-On Password (Hasło uruchomieniowe)**, a następnie postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.
4. Przed wyjściem z programu kliknij kolejno **File (Plik) > Save Changes and Exit (Zapisz zmiany i zakończ)**.



## Wprowadzanie hasła uruchomieniowego

Aby wprowadzić hasło uruchomieniowe, wykonaj następujące czynności:

1. Włącz lub uruchom ponownie komputer. W systemie Windows kliknij kolejno **Start > Zamknij > Uruchom ponownie komputer**.
2. Po pojawieniu się ikony klucza wpisz bieżące hasło, a następnie naciśnij klawisz **Enter**.



Hasło należy wpisywać uważnie, ponieważ ze względów bezpieczeństwa znaki nie są wyświetlane na ekranie.

Jeżeli zostanie podane nieprawidłowe hasło, na ekranie pojawi się ikona przedstawiająca przełamany klucz. Należy spróbować ponownie wpisać poprawne hasło. Po trzech nieudanych próbach wprowadzenia hasła komputer należy wyłączyć, a następnie włączyć i ponownie wprowadzić hasło.

## Wprowadzanie hasła konfiguracyjnego

Jeśli system jest wyposażony we wbudowany mikroukład zabezpieczeń, należy zapoznać się z informacjami w *Podręczniku oprogramowania HP ProtectTools Security Manager* w witrynie [www.hp.com](http://www.hp.com).

Jeżeli ustawiono hasło konfiguracyjne komputera, jego podanie będzie wymagane przy każdej próbie uruchomienia programu Computer Setup.

1. Włącz lub uruchom ponownie komputer. W systemie Windows kliknij kolejno **Start > Zamknij > Uruchom ponownie**.
2. Zaraz po włączeniu komputera, gdy dioda zasilania monitora zaświeci się na zielono, naciśnij klawisz **F10**, aby otworzyć program Computer Setup. W razie potrzeby możesz nacisnąć klawisz **Enter**, aby pominąć ekran tytułowy.



Jeśli klawisz **F10** nie zostanie naciśnięty w odpowiednim czasie, dostęp do programu będzie możliwy dopiero po ponownym uruchomieniu komputera, a następnie ponownym naciśnięciu klawisza **F10**, gdy dioda zasilania monitora zaświeci się na zielono.

3. Po pojawieniu się ikony klucza wpisz hasło konfiguracyjne, a następnie naciśnij klawisz **Enter**.



Hasło należy wpisywać uważnie, ponieważ ze względów bezpieczeństwa znaki nie są wyświetlane na ekranie.

Jeżeli zostanie podane nieprawidłowe hasło, na ekranie pojawi się ikona przedstawiająca przelamany klucz. Należy spróbować ponownie wpisać poprawne hasło. Po trzech nieudanych próbach wprowadzenia hasła komputer należy wyłączyć, a następnie włączyć i ponownie wprowadzić hasło.

## Zmiana hasła uruchomieniowego lub konfiguracyjnego

Jeśli system jest wyposażony we wbudowany mikroukład zabezpieczeń, należy zapoznać się z informacjami w *Podręczniku oprogramowania HP ProtectTools Security Manager* w witrynie [www.hp.com](http://www.hp.com).

1. Włącz lub uruchom ponownie komputer. W systemie Windows kliknij kolejno **Start > Zamknij > Uruchom ponownie komputer**.
2. Aby zmienić hasło uruchomieniowe, przejdź do punktu 3.

Aby zmienić hasło konfiguracyjne, zaraz po włączeniu komputera naciśnij i przytrzymaj klawisz **F10**, gdy dioda monitora zaświeci się na zielono, aby otworzyć program Computer Setup. W razie potrzeby możesz nacisnąć klawisz **Enter**, aby pominąć ekran tytułowy.



Jeśli klawisz **F10** nie zostanie naciśnięty w odpowiednim czasie, dostęp do programu będzie możliwy dopiero po ponownym uruchomieniu komputera, a następnie ponownym naciśnięciu klawisza **F10**, gdy dioda zasilania monitora zaświeci się na zielono.

3. Po pojawieniu się ikony klucza wpisz bieżące hasło, a następnie dwa razy nowe hasło, rozdzielając je znakiem ukośnika (/) lub innym separatorem, zgodnie ze wzorem:  
**bieżące hasło/nowe hasło/nowe hasło**



Hasło należy wpisywać uważnie, ponieważ ze względów bezpieczeństwa znaki nie są wyświetlane na ekranie.

---

4. Naciśnij klawisz **Enter**.

Nowe hasło zacznie obowiązywać po następnym włączeniu komputera.

---



Informacje na temat innych separatorów można znaleźć w części „Separatory dla różnych układów klawiatury” na stronie 40. Hasła uruchomieniowe i konfiguracyjne można również zmieniać przy użyciu opcji menu Security (Zabezpieczenia) w programie Computer Setup.

---

## Usuwanie hasła uruchomieniowego lub konfiguracyjnego

Jeśli system jest wyposażony we wbudowany mikroukład zabezpieczeń, należy zapoznać się z informacjami w *Podręczniku oprogramowania HP ProtectTools Security Manager* w witrynie [www.hp.com](http://www.hp.com).

1. Włącz lub uruchom ponownie komputer. W systemie Windows kliknij kolejno **Start > Zamknij > Uruchom ponownie komputer**.

2. Aby usunąć hasło uruchomieniowe, przejdź do punktu 3.

Aby usunąć hasło konfiguracyjne, zaraz po włączeniu komputera naciśnij i przytrzymaj klawisz **F10**, gdy dioda monitora zaświeci się na zielono, aby otworzyć program Computer Setup. W razie potrzeby możesz nacisnąć klawisz **Enter**, aby pominąć ekran tytułowy.

---



Jeśli klawisz **F10** nie zostanie naciśnięty w odpowiednim czasie, dostęp do programu będzie możliwy dopiero po ponownym uruchomieniu komputera, a następnie ponownym naciśnięciu klawisza **F10**, gdy dioda zasilania monitora zaświeci się na zielono.

---

3. Po pojawieniu się ikony klucza wpisz bieżące hasło, a następnie znak ukośnika (/) lub inny separator, zgodnie ze wzorem:  
**bieżące hasło/**

4. Naciśnij klawisz **Enter**.



Informacje na temat innych separatorów można znaleźć w części „[Separatory dla różnych układów klawiatury](#)”. Hasła uruchomieniowe i konfiguracyjne można również zmieniać przy użyciu opcji menu Security (Zabezpieczenia) w programie Computer Setup.

## Separatory dla różnych układów klawiatury

Konstrukcja każdej klawiatury uwzględnia wymagania specyficzne dla danego języka. Z tego względu separatory oraz klawisze używane podczas zmiany lub usuwania hasła zależą od typu klawiatury dołączonej do komputera.

### Separatory dla różnych układów klawiatury

angielska (USA)	/	grecka	-	portugalska	-
angielska (Wielka Brytania)	/	hebrajska	.	rosyjska	/
arabska	/	hiszpańska	-	słowacka	-
belgijska	=	chińska	/	szwajcarska	-
BHCSY*	-	japońska	/	szwedzka/ fińska	/
brazylijska	/	koreańska	/	tajska	/
czeska	-	Niemcy	-	tajwańska	/
duńska	-	norweska	-	turecka	.
francuska	!	polska	-	węgierska	-
francuska (Kanada)	é	południowo- amerykańska	-	włoska	-

\* dotyczy Bośni-Hercegowiny, Chorwacji, Słowenii i Jugosławii

## Czyszczenie haseł

Utrata hasła uniemożliwia dostęp do komputera. W *Podręczniku rozwiązywania problemów* na dysku CD *Dokumentacja i diagnostyka* można znaleźć instrukcje dotyczące czyszczenia haseł.

Jeśli system jest wyposażony we wbudowany mikroukład zabezpieczeń, należy zapoznać się z informacjami w *Podręczniku oprogramowania HP ProtectTools Security Manager* w witrynie [www.hp.com](http://www.hp.com).

## Blokada DriveLock

DriveLock to będąca standardem przemysłowym funkcja zabezpieczeń, która zapobiega nieautoryzowanemu dostępowi do danych przechowywanych na dyskach twardych ATA. Funkcja ta jest zaimplementowana jako rozszerzenie programu Computer Setup. Jest ona dostępna tylko po wykryciu w systemie dysków twardych obsługujących zestaw poleceń ATA Security. Funkcja DriveLock została opracowana z myślą o klientach firmy HP, dla których bezpieczeństwo danych jest sprawą priorytetową. Chodzi o klientów, dla których całkowity koszt dysku twardego i danych na nim przechowywanych (w przypadku ich utraty) jest nieporównywalnie mniejszy od strat, jakie może spowodować dostęp do tych danych przez osoby niepowołane. W celu uzyskania kompromisu między wymaganym poziomem zabezpieczeń i koniecznością dostępu do danych w przypadku utraty hasła implementacja funkcji DriveLock wykorzystuje schemat zabezpieczeń oparty na dwóch hasłach. Pierwsze z nich jest ustawiane i stosowane przez administratora systemu, drugie natomiast — przez użytkownika końcowego. Jeżeli oba hasła zostaną utracone, dostęp do dysku zostanie całkowicie zablokowany. Dlatego też w celu zwiększenia bezpieczeństwa związanego ze stosowaniem funkcji DriveLock zalecane jest replikowanie lub tworzenie kopii zapasowych danych przechowywanych na dysku w wewnętrznym systemie informacyjnym przedsiębiorstwa. W przypadku utraty obu haseł używanie zabezpieczonego dysku jest niemożliwe. W praktyce oznacza to utratę całego dysku wraz z zawartymi na nim danymi, co może być problemem dla wielu użytkowników. Jednak dla użytkowników wspomnianych na początku tej części (tzn. ceniących sobie bezpieczeństwo danych) ryzyko utraty dysku i danych bez możliwości ich odczytania przez osoby nieupoważnione jest do przyjęcia.

## Korzystanie z funkcji DriveLock

Opcja DriveLock jest dostępna w menu Security (Zabezpieczenia) programu Computer Setup. W tym menu możliwe jest ustawienie hasła głównego lub włączenie funkcji DriveLock. Jeżeli funkcja DriveLock ma zostać włączona, należy podać hasło użytkownika. Ponieważ funkcja ta jest zwykle najpierw konfigurowana przez administratora systemu, jako pierwsze musi zostać ustawione hasło główne. Ustawienie tego hasła jest zalecane, jeżeli planowane jest włączenie funkcji DriveLock, jak również jeżeli funkcja ta nie ma być używana. Umożliwi to administratorowi zmianę ustawień tej opcji w przypadku zablokowania dysku w przyszłości. Po ustawieniu hasła administrator systemu może włączyć funkcję DriveLock lub pozostawić ją wyłączoną.

Jeżeli w systemie zostanie wykryty zablokowany dysk twardy, podczas autotestu POST konieczne będzie podanie odpowiedniego hasła. Jeżeli ustawione jest hasło uruchomieniowe i jest ono takie samo, jak hasło użytkownika urządzenia, podczas autotestu POST nie pojawi się monit o wprowadzenie hasła. W przeciwnym wypadku użytkownik otrzyma monit o podanie hasła funkcji DriveLock. Można wprowadzić również hasło główne. Użytkownik może podjąć dwie próby wprowadzenia poprawnego hasła. Jeżeli odpowiednie hasło nie zostanie wprowadzone, autotest POST będzie kontynuowany, ale zablokowany dysk będzie niedostępny.

## Zastosowania funkcji DriveLock

Najbardziej praktycznym zastosowaniem funkcji zabezpieczeń DriveLock jest korzystanie z niej w środowisku korporacyjnym. Administrator systemu jest odpowiedzialny za skonfigurowanie dysku twardego, co jest między innymi związane z ustawieniem hasła głównego funkcji DriveLock. W przypadku utraty hasła użytkownika lub przekazania komputera innemu pracownikowi zmiana hasła użytkownika i uzyskanie ponownego dostępu do dysku są możliwe za pomocą hasła głównego.

Firma HP zaleca, aby administratorzy systemu w przedsiębiorstwach, w których stosowana jest funkcja DriveLock, ustanowili ogólne zasady dotyczące ustawiania i obsługi haseł głównych. Jeżeli zasady te nie zostaną ustanowione, może wystąpić sytuacja, w której oba hasła funkcji zostaną ustawione (celowo bądź przez przypadek) przez pracownika na krótko przed zakończeniem jego zatrudnienia (np. z powodu zwolnienia lub przejścia na emeryturę). Po odejściu pracownika zablokowany przez niego dysk nie będzie mógł być używany i konieczna będzie jego wymiana. Podobnie jeżeli administrator nie ustawi hasła głównego, może nie być możliwe przeprowadzenie sprawdzenia zainstalowanego oprogramowania oraz obsługa innych funkcji kontroli dostępu.

Włączanie funkcji DriveLock nie jest zalecane w przypadku użytkowników, których wymagania dotyczące bezpieczeństwa danych nie są tak wysokie. Kategoria ta obejmuje użytkowników indywidualnych oraz użytkowników, którzy nie przechowują zwykle na swoich dyskach poufnych danych. Dla tych użytkowników ostateczne zablokowanie dysku spowodowane utratą obu haseł funkcji DriveLock jest znacznie bardziej kosztowne niż ewentualne ujawnienie zapisanych na nim danych. Dostęp do opcji DriveLock (i programu Computer Setup) może zostać ograniczony przy użyciu hasła konfiguracyjnego. Przez określenie hasła konfiguracyjnego i zablokowanie dostępu do niego przez użytkowników końcowych, administratorzy systemów mogą ograniczyć użytkownikom możliwość włączania funkcji DriveLock.

## Czujnik Smart Cover Sensor

Cover Removal Sensor to dostępna w niektórych modelach komputera funkcja będąca połączeniem technologii sprzętowych i programowych, która może wysyłać alerty informujące o zdjęciu pokrywy lub panelu dostępu komputera. Czujnik ten oferuje trzy poziomy zabezpieczeń, opisane w poniższej tabeli.

## Poziomy zabezpieczeń czujnika Smart Cover Sensor

Poziom	Ustawienie	Opis
Poziom 0	Disabled (Wyłączone)	Czujnik Smart Cover Sensor jest wyłączony (ustawienie domyślne)
Poziom 1	Notify User (Powiadamianie użytkownika)	Po ponownym uruchomieniu komputera na ekranie pojawi się komunikat informujący o zdjęciu pokrywy lub panelu bocznego komputera.
Poziom 2	Setup Password (Hasło konfiguracyjne)	Po ponownym uruchomieniu komputera na ekranie pojawi się komunikat informujący o zdjęciu pokrywy lub panelu bocznego komputera. Aby kontynuować, należy wprowadzić hasło konfiguracyjne.



Ustawienia te można zmieniać w programie Computer Setup. Więcej informacji o programie Computer Setup można znaleźć w *Podręczniku do programu Computer Setup (F10)* na dysku CD *Dokumentacja i diagnostyka*.

## Ustawianie poziomów zabezpieczeń czujnika Smart Cover Sensor

Aby ustawić poziom zabezpieczeń czujnika Smart Cover Sensor, wykonaj poniższe czynności:

1. Włącz lub uruchom ponownie komputer. W systemie Windows kliknij kolejno **Start > Zamknij > Uruchom ponownie**.
2. Zaraz po włączeniu komputera, gdy dioda zasilania monitora zaświeci się na zielono, naciśnij klawisz **F10**, aby otworzyć program Computer Setup. W razie potrzeby możesz nacisnąć klawisz **Enter**, aby pominąć ekran tytułowy.



Jeśli klawisz **F10** nie zostanie naciśnięty w odpowiednim czasie, dostęp do programu będzie możliwy dopiero po ponownym uruchomieniu komputera, a następnie ponownym naciśnięciu klawisza **F10**, gdy dioda zasilania monitora zaświeci się na zielono.

3. Wybierz kolejno **Security (Zabezpieczenia) > Smart Cover (Pokrywa inteligentna) > Cover Removal Sensor (Czujnik zdjęcia pokrywy)**, a następnie wybierz żądany poziom zabezpieczeń.
4. Przed wyjściem z programu kliknij kolejno **File (Plik) > Save Changes and Exit (Zapisz zmiany i zakończ)**.



## Smart Cover Lock

Smart Cover Lock jest sterowaną programowo blokadą pokrywy komputera dostępną w niektórych komputerach firmy HP. Zapobiega ona nieautoryzowanemu dostępowi do wewnętrznych elementów komputera. Komputer jest dostarczany z wyłączoną blokadą SmartCover Lock.



**PRZESTROGA:** Aby zabezpieczyć ustawienia blokady SmartCover Lock, należy pamiętać o ustawieniu hasła konfiguracyjnego. Hasło to zapobiega nieautoryzowanemu dostępowi do programu Computer Setup.



Blokada Smart Cover Lock jest dostępna jako opcja w niektórych systemach.

## Włączanie blokady Smart Cover Lock

Aby włączyć blokadę Smart Cover Lock, wykonaj poniższe czynności:

1. Włącz lub uruchom ponownie komputer. W systemie Windows kliknij kolejno **Start** > **Zamknij** > **Uruchom ponownie**.
2. Zaraz po włączeniu komputera, gdy dioda zasilania monitora zaświeci się na zielono, naciśnij klawisz **F10**, aby otworzyć program Computer Setup. W razie potrzeby możesz nacisnąć klawisz **Enter**, aby pominąć ekran tytułowy.



Jeśli klawisz **F10** nie zostanie naciśnięty w odpowiednim czasie, dostęp do programu będzie możliwy dopiero po ponownym uruchomieniu komputera, a następnie ponownym naciśnięciu klawisza **F10**, gdy dioda zasilania monitora zaświeci się na zielono.

3. Wybierz kolejno **Security (Zabezpieczenia)** > **Smart Cover (Pokrywa inteligentna)** > **Cover Lock (Blokada pokrywy)** > **Lock (Zablokuj)**.
4. Przed wyjściem z programu kliknij kolejno **File (Plik)** > **Save Changes and Exit (Zapisz zmiany i zakończ)**.

## Wyłączanie blokady Smart Cover Lock

1. Włącz lub uruchom ponownie komputer. W systemie Windows kliknij kolejno **Start > Zamknij > Uruchom ponownie**.
2. Zaraz po włączeniu komputera, gdy dioda zasilania monitora zaświeci się na zielono, naciśnij klawisz **F10**, aby otworzyć program Computer Setup. W razie potrzeby możesz nacisnąć klawisz **Enter**, aby pominąć ekran tytułowy.



Jeśli klawisz **F10** nie zostanie naciśnięty w odpowiednim czasie, dostęp do programu będzie możliwy dopiero po ponownym uruchomieniu komputera, a następnie ponownym naciśnięciu klawisza **F10**, gdy dioda zasilania monitora zaświeci się na zielono.

3. Wybierz kolejno **Security (Zabezpieczenia) > Smart Cover (Pokrywa inteligentna) > Cover Lock (Blokada pokrywy) > Unlock (Odblokuj)**.
4. Przed wyjściem z programu kliknij kolejno **File (Plik) > Save Changes and Exit (Zapisz zmiany i zakończ)**.

## Używanie klucza Smart Cover FailSafe Key

Jeżeli włączona jest blokada Smart Cover Lock i z różnych powodów nie można wprowadzić wyłączającego ją hasła konfiguracyjnego, pokrywę komputera można otworzyć za pomocą klucza Smart Cover FailSafe Key. Sytuacje, w których niezbędne jest użycie klucza to:

- brak zasilania,
- błąd podczas uruchamiania komputera,
- wadliwe elementy komputera (np. wadliwy procesor lub zasilacz),
- utrata hasła.



**PRZESTROGA:** Klucz Smart Cover FailSafe Key jest specjalistycznym narzędziem dostępnym w firmie HP. Ze względu na duże prawdopodobieństwo wystąpienia wymienionych wcześniej sytuacji, klucz taki najlepiej zamówić odpowiednio wcześniej u autoryzowanego sprzedawcy lub serwisanta.

Aby nabyć klucz FailSafe Key, należy:

- Skontaktować się z autoryzowanym sprzedawcą lub serwisantem produktów firmy HP.
- Zadzwoić pod odpowiedni numer wskazany w gwarancji.

Więcej informacji dotyczących korzystania z klucza Smart Cover FailSafe Key można znaleźć w *Instrukcji obsługi sprzętu* na dysku CD *Dokumentacja i diagnostyka*.

## Zabezpieczająca blokada kablowa

Z tyłu komputera znajduje się gniazdo blokady kablowej, umożliwiające przymocowanie komputera do nieruchomego obiektu przy stanowisku pracy.

Szczegółowe instrukcje (wraz z rysunkami) można znaleźć w *Instrukcji obsługi sprzętu* na dysku CD *Dokumentacja i diagnostyka*.

## Identyfikacja na podstawie analizy linii papilarnych

Dzięki wprowadzeniu opracowanej przez firmę HP technologii identyfikacji użytkownika na podstawie analizy linii papilarnych przestaje być konieczne wprowadzanie haseł, a tym samym podnosi się poziom bezpieczeństwa w sieci, uproszczeniu ulega proces logowania, a także obniżają się koszty związane z zarządzaniem siecią komputerową przedsiębiorstwa. Rozwiązanie to stało się dostępne po atrakcyjnej cenie dla wielu przedsiębiorstw, nie tylko tych wysoko zaawansowanych technologicznie i korzystających z rozbudowanych systemów zabezpieczeń.



W zależności od modelu technologia ta jest wykorzystywana w różny sposób.

---

Więcej informacji można znaleźć na stronie:

<http://h18004.www1.hp.com/products/security/>.

## Powiadamianie o usterkach i ich usuwanie

Funkcja powiadamiania o usterkach i ich usuwania łączy w sobie zalety nowoczesnej technologii sprzętowej i programowej, dzięki czemu znacznie obniża ryzyko utraty istotnych danych oraz wystąpienia nieplanowanych przestojów w pracy.

Jeśli komputer jest podłączony do sieci pracującej pod kontrolą programu HP Client Manager, powiadomienie o usterce jest przesyłane do tej aplikacji. Za pomocą programu HP Client Manager Software można też zdalnie planować automatyczne uruchamianie diagnostyki na wszystkich zarządzanych komputerach i tworzyć raporty podsumowujące dotyczące testów, które zakończyły się niepowodzeniem.

## System ochrony dysków

System ochrony dysków Drive Protection System (DPS) jest narzędziem diagnostycznym, zintegrowanym z dyskami twardymi instalowanymi w niektórych komputerach HP. System ten ułatwia diagnozowanie problemów, w wyniku których mogłaby zaistnieć potrzeba nieobjętej gwarancją wymiany dysku twardego.

Podczas montażu komputerów firmy HP każdy instalowany w nich dysk twardy jest testowany przy użyciu programu DPS, a kluczowe informacje są na nim zapisywane na stałe. Każdorazowe uruchomienie programu DPS powoduje zapisanie wygenerowanych przez niego wyników na dysku twardym. Informacje te mogą pomóc serwisantowi w zdiagnozowaniu warunków, które spowodowały uruchomienie oprogramowania DPS. Informacje dotyczące używania systemu DPS znajdują się w *Podręczniku rozwiązywania problemów* na dysku CD *Dokumentacja i diagnostyka*.

## Zasilacz z zabezpieczeniem antyprzepięciowym

Zintegrowany zasilacz z zabezpieczeniem antyprzepięciowym zapewnia większą niezawodność pracy komputera w przypadku wystąpienia gwałtownych zmian napięcia w sieci. Bez ryzyka utraty danych i przestojów systemu wytrzymuje on skoki napięcia do 2000 V.

## Czujnik termiczny

Czujnik termiczny, łącząc w sobie funkcje programowe i sprzętowe, jest urządzeniem rejestrującym temperaturę wewnątrz komputera. W momencie przekroczenia dopuszczalnej temperatury wyświetlany jest odpowiedni komunikat. Dzięki odpowiednio wczesnemu ostrzeżeniu użytkownik może podjąć odpowiednie kroki, które zapobiegą uszkodzeniu komputera i utracie danych.

---

# Indeks

## A

adresy internetowe, zobacz  
    witryny sieci Web  
adresy URL (witryny sieci Web), zobacz  
    witryny sieci Web  
Altiris 7  
    AClient 3  
    Deployment Solution Agent 3

## B

blokada Smart Cover Lock, włączanie 45

## C

Computer Setup 18  
cover lock, smart 45  
czujnik termiczny 49  
czyszczenie 40  
czyszczenie haseł 40

## D

Dantz Retrospect Express 12  
DiskOnKey  
    *zobacz też* HP Drive Key  
    rozruchowe 21–26  
dostęp do komputera, kontrolowanie 29  
dostosowywanie oprogramowania 2  
Drivelock 41–43  
dwufunkcyjny przycisk zasilania 27  
dysk, klonowanie 2  
dysk, ochrona 48  
dyski twarde, narzędzie diagnostyczne 48

## F

FailSafe Key  
    przestrogi 46  
    zamawianie 47

## H

hasło 40  
    konfiguracyjne 35, 37  
    uruchomieniowe 37  
    usuwanie 39  
    zabezpieczenie 34  
    zmiana 38  
hasło konfiguracyjne  
    ustawianie 35  
    usuwanie 39  
    wprowadzanie 37  
    zmiana 38  
hasło uruchomieniowe  
    usuwanie 39  
    wprowadzanie 37  
    zmiana 38  
HP Client Management Solutions 7  
HP Client Manager Software 6  
HP Drive Key  
    *zobacz też* DiskOnKey  
    rozruchowe 21–26  
HP Lifecycle solutions 2  
HP Local Recovery 10  
HP OpenView Management Suite for  
    Desktops Using Radia 9  
HP System Software Manager 5

**I**

identyfikacja na podstawie analizy linii papilarnych 47

**K**

klucz Smart Cover FailSafe Key, zamawianie 47

konfiguracja  
  replikowanie 18

konfigurowanie  
  początkowe 2

konfigurowanie przycisku zasilania 27

kontrolowanie dostępu do komputera 29

**L**

Local Recovery 3

**N**

narzędzia klonowania, oprogramowanie 2

narzędzia rozmieszczania,  
  oprogramowanie 2

narzędzie diagnostyczne dla dysków  
  twardych 48

**O**

ochrona dysku twardego 48

odzyskiwanie, oprogramowanie 2

oprogramowanie 29

  aktualizowanie i zarządzanie 5

  Altiris AClient 3

  Altiris Deployment Solution Agent 3

  Computer Setup 18

  Drive Protection System 48

  HP Local Recovery 3

  integracja 2

  odzyskiwanie 2

  powiadamianie o usterkach i ich  
  usuwanie 48

  zdalne instalowanie systemu 4

  zdalne zarządzanie pamięcią ROM typu  
  flash 16

**P**

PCN (Proactive Change Notification) 13

początkowa konfiguracja 2

powiadamianie o usterkach 48

powiadomienia o zmianach 13

powiadomienie o zmianie 13

Preboot Execution Environment (PXE) 4

preinstalowany obraz oprogramowania 2

Proactive Change Notification (PCN) 13

przestrogi

  FailSafe Key 46

  zabezpieczanie pamięci ROM 15

  zabezpieczenie blokady

    Smart Cover Lock 45

przycisk zasilania

  dwufunkcyjny 27

  konfigurowanie 27

PXE (Preboot Execution Environment) 4

**R**

ROM

  flash 15

  Zdalne zarządzanie pamięcią typu

    flash 16

rozmieszczanie komputerów 2

**S**

separatory klawiatury, narodowe 40

separatory różnych klawiatur 40

separatory, tabela 40

Smart Cover Lock 45–47

  wyłączanie 46

Smart Cover Sensor 43

  poziomy zabezpieczeń 44

  ustawianie 44

Subscriber's Choice 14

systemy operacyjne, ważne informacje 28

**Ś**

śledzenie majątku 29

śledzenie zasobów 29

**T**

temperatura wewnętrzna komputera 49

**U**

urządzenie rozruchowe

    DiskOnKey 21–26

    HP Drive Key 21–26

    tworzenie 21–26

    urządzenie USB typu flash 21–26

urządzenie USB typu flash,

    rozruchowe 21–26

usuwanie hasła 39

**W**

włączanie blokady Smart Cover Lock 45

wewnętrzna temperatura komputera 49

witryny sieci Web

    HPQFlash 16

    identyfikacja na podstawie analizy linii  
    papilarnych 47

    obsługa oprogramowania 28

    pamięć ROM typu flash 15

    Proactive Change Notification 13

    replikowanie ustawień

        konfiguracyjnych 20, 21

    rozmieszczanie komputera 2

    Subscriber's Choice 14

    zdalne zarządzanie pamięcią ROM typu  
    flash 16

wprowadzanie

    hasło konfiguracyjne 37

    hasło uruchomieniowe 37

wyłączanie blokady Smart Cover Lock 46

wycofane rozwiązania 14

**Z**

zabezpieczająca blokada kablowa 47

zabezpieczanie Multibay 41–43

zabezpieczanie pamięci ROM, przestroga 15

zabezpieczenia

    DriveLock 41–43

    funkcje, tabela 31

    MultiBay 41–43

    Smart Cover Lock 45–47

    Smart Cover Sensor 43

    ustawienia, konfigurowanie 29

zabezpieczenie

    hasłem 34

zabezpieczenie antyprzebieciowe,

    zasilacz 48

zabezpieczenie blokady Smart Cover Lock,  
    przestroga 45

zamawianie klucza FailSafe Key 47

zasilacz, z zabezpieczeniem

    antyprzebieciowym 48

zdalna instalacja 4

Zdalne instalowanie systemu

    uzyskiwanie dostępu 4

zdalne instalowanie systemu 4

zdalne zarządzanie pamięcią ROM typu  
    flash 16

zmiana hasła 38

zmiana systemów operacyjnych, ważne  
    informacje 28